

IN THE CLAIMS

1. (Currently Amended) An apparatus for executing authentication in a network environment, comprising:

a packet gateway operable to retrieve a group profile from an authentication, authorization, and accounting (AAA) server in response to receiving a request from a first end user and to locally cache the group profile, **wherein the packet gateway determines if the first end user is authenticated and if the first end user is unauthenticated, then the packet gateway searches a local cache for a profile with network digits of the first end user's MSID, whereby if the profile is not in the local cache or has expired, then the packet gateway purges the expired profile or requests the profile from the AAA server, caches the profile, and marks an expiry time that is provided within the profile, once the profile is in the cache, subsequent users that belong to a same group can be authorized with a realm and with authorization attributes and without involving the AAA server,** the packet gateway being operable to provide a service to the first end user based on information included within the group profile and associated with the first end user, wherein the packet gateway is further operable to receive a request from a second end user and to determine if the second end user is included within the group profile such that in cases where the second end user is included in the group profile the packet gateway can locally cache the group profile in order to provide a service to the second end user without having to communicate with the AAA server.

2. (Original) The apparatus of Claim 1, wherein the group profile includes a plurality of end users that share a common prefix associated with their mobile station identifiers (MSIDs).

3. (Original) The apparatus of Claim 1, wherein if the second end user is not in the group profile associated with the first end user, then the packet gateway may initiate a request to the AAA server in order to attempt to identify a profile associated with the second end user.

4. (Original) The apparatus of Claim 1, wherein if the group profile associated with first end user has expired, the packet gateway may initiate a request to the AAA server for a valid profile that corresponds to the first end user.

5. (Original) The apparatus of Claim 1, wherein each group profile includes an expiration time such that if the group profile is identified as having expired, it may be expunged.

6. (Original) The apparatus of Claim 1, further comprising:
a centralized server operable to store a plurality of group profiles and to return requested group profiles to the packet gateway so that they can be locally cached.

7. (Original) The apparatus of Claim 1, wherein the packet gateway includes a table operable to store one or more group profiles that may be locally cached.

8. (Currently Amended) A method for executing authentication in a network environment, comprising:

retrieving a group profile from an authentication, authorization, and accounting (AAA) server in response to receiving a request from a first end user;

locally caching the group profile;

providing a service to the first end user based on information included within the group profile and associated with the first end user, **wherein the packet gateway determines if the first end user is authenticated and if the first end user is unauthenticated, then the packet gateway searches a local cache for a profile with network digits of the first end user's MSID, whereby if the profile is not in the local cache or has expired, then the packet gateway purges the expired profile or requests the profile from the AAA server, caches the profile, and marks an expiry time that is provided within the profile, once the profile is in the cache, subsequent users that belong to a same group can be authorized with a realm and with authorization attributes and without involving the AAA server;**

receiving a request from a second end user; and
determining if the second end user is included within the group profile such that in cases where the second end user is included in the group profile the group profile can be locally cached in order to provide a service to the second end user without having to communicate with the AAA server.

9. (Original) The method of Claim 8, wherein the group profile includes a plurality of end users that share a common prefix associated with their mobile station identifiers (MSIDs).

10. (Original) The method of Claim 8, wherein if the second end user is not in the group profile associated with the first end user, then a request is communicated to the AAA server in order to attempt to identify a profile associated with the second end user.

11. (Original) The method of Claim 8, wherein if the group profile associated with first end user has expired, a request may be communicated to the AAA server for a valid profile that corresponds to the first end user.

12. (Original) The method of Claim 8, further comprising:
storing a plurality of group profiles; and
returning requested group profiles such that they can be locally cached.

13. (Currently Amended) A system for executing authentication in a network environment, comprising:

means for retrieving a group profile from an authentication, authorization, and accounting (AAA) server in response to receiving a request from a first end user;

means for locally caching the group profile;

means for providing a service to the first end user based on information included within the group profile and associated with the first end user, wherein the packet gateway determines if the first end user is authenticated and if the first end user is unauthenticated, then the packet gateway searches a local cache for a profile with network digits of the first end user's MSID, whereby if the profile is not in the local cache or has expired, then the packet gateway purges the expired profile or requests the profile from the AAA server, caches the profile, and marks an expiry time that is provided within the profile, once the profile is in the cache, subsequent users that belong to a same group can be authorized with a realm and with authorization attributes and without involving the AAA server;

means for receiving a request from a second end user; and

means for determining if the second end user is included within the group profile such that in cases where the second end user is included in the group profile the group profile can be locally cached in order to provide a service to the second end user without having to communicate with the AAA server.

14. (Original) The system of Claim 13, wherein the group profile includes a plurality of end users that share a common prefix associated with their mobile station identifiers (MSIDs).

15. (Original) The system of Claim 13, wherein if the second end user is not in the group profile associated with the first end user, then a request is communicated to the AAA server in order to attempt to identify a profile associated with the second end user.

16. (Original) The system of Claim 13, wherein if the group profile associated with first end user has expired, a request may be communicated to the AAA server for a valid profile that corresponds to the first end user.

17. (Original) The system of Claim 13, further comprising:

means for storing a plurality of group profiles; and

means for returning requested group profiles such that they can be locally cached.

18. (Currently Amended) Software for executing authentication in a network environment, the software being embodied in a computer readable medium and comprising computer code such that when executed is operable to:

retrieve a group profile from an authentication, authorization, and accounting (AAA) server in response to receiving a request from a first end user;

locally cache the group profile;

provide a service to the first end user based on information included within the group profile and associated with the first end user, **wherein the packet gateway determines if the first end user is authenticated and if the first end user is unauthenticated, then the packet gateway searches a local cache for a profile with network digits of the first end user's MSID, whereby if the profile is not in the local cache or has expired, then the packet gateway purges the expired profile or requests the profile from the AAA server, caches the profile, and marks an expiry time that is provided within the profile, once the profile is in the cache, subsequent users that belong to a same group can be authorized with a realm and with authorization attributes and without involving the AAA server;**

receive a request from a second end user; and

determine if the second end user is included within the group profile such that in cases where the second end user is included in the group profile the group profile can be locally cached in order to provide a service to the second end user without having to communicate with the AAA server.

19. (Original) The computer readable medium of Claim 18, wherein the group profile includes a plurality of end users that share a common prefix associated with their mobile station identifiers (MSIDs).

20. (Original) The computer readable medium of Claim 18, wherein if the second end user is not in the group profile associated with the first end user, then a request is communicated to the AAA server in order to attempt to identify a profile associated with the second end user.

21. (Original) The computer readable medium of Claim 18, wherein if the group profile associated with first end user has expired, a request may be communicated to the AAA server for a valid profile that corresponds to the first end user.

22. (Original) The computer readable medium of Claim 18, wherein in the code is further operable to:

store a plurality of group profiles; and

return requested group profiles such that they can be locally cached.